Duadic Group Algebra Codes

Salah A. Aly, Andreas Klappenecker, Pradeep Kiran Sarvepalli

Department of Computer Science, Texas A&M University
College Station, TX 77843-3112, USA
Email: {salah, klappi, pradeep}@cs.tamu.edu

Abstract— **Duadic group algebra codes are a generalization of quadratic residue codes. This paper settles an open problem raised by Zhu concerning the existence of duadic group algebra codes. These codes can be used to construct degenerate quantum stabilizer codes that have the nice feature that many errors of small weight do not need error correction; this fact is illustrated by an example.**

I. INTRODUCTION

Binary cyclic duadic codes were introduced by Leon, Masley and Pless [5] as a generalization of quadradic residue codes. Duadic codes share many properties of quadratic residue codes, but are more flexible; for example, they are not restricted to prime lengths. Subsequently, cyclic duadic code were generalized to nonbinary fields in [7], [9], [10]. Further progress was made by interpreting duadic codes as group algebra codes in the sense of MacWilliams [6]. Using this point of view, duadic codes were extended to abelian groups by Rushanan [7] and to nonabelian group by Zhu [14]. In this paper, we further relax the requirements and allow for a wider class of antiautomorphisms.

An open problem by Zhu [14] asks to find necessary and sufficient conditions for the existence of duadic group algebra codes with splitting given by μ_{-1} (the terminology is explained in the next section). Partial answers to this question were obtained by Smid [10] in the cyclic case, by Ward and Zhu [12] and Rushanan [7] in the abelian case, and by Zhang [13] in the case of (nonabelian) finite groups and finite fields of characteristic 2.

The main result of this paper settles Zhu's question in the general case of arbitrary finite groups and arbitrary finite fields. We show that if G is a finite group of odd order n and $\mathbf{F}_q$ is a finite field with q elements such that $\gcd(q,n) = 1$, then there exists a splitting given by μ_{-1} with central idempotents e and f if and only if the order of q is odd modulo n. In our proof, we establish a key proposition that allows us to transfer the existence question of duadic group algebra codes (for an arbitrary splitting) to a question about so-called $\mathbf{F}_q$-conjugacy classes of the group. Furthermore, we give an example for the existence of a splitting μ when μ_{-1}-splitting cannot exist.

One of the applications of duadic group algebra codes is the construction of (degenerate) quantum error-correcting codes; here duadic group algebra codes can provide even better results than cyclic duadic codes, but space constraints will only allow us to sketch an example. We derive a family of quantum codes with parameters $[[n, 1, d]]_q$ such that $d^2 - d + 1 \geq n$.

II. DUADIC GROUP ALGEBRA CODES

A. Background

Let G be a finite group of order n with identity element 1 and let $\mathbf{F}_q$ denote a finite field with q elements such that $\gcd(q,n) = 1$. Recall that the group algebra $R = \mathbf{F}_q[G]$ consists of elements of the form $\sum_{g \in G} a_g g$, with $a_g \in \mathbf{F}_q$. The set R is a vector space over $\mathbf{F}_q$ in which the elements of G form a basis. Furthermore, R is equipped with a multiplication defined by the convolutional product

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \left(\sum_{h \in G} a_h b_{h^{-1}g} \right) g.$$

A left ideal in R is an additive subgroup I of R such that $ra \in I$ for all r in R and a in I. A *group algebra code* in R, or shortly an R-code, is a left ideal I of R.

For example, if $G = \mathbf{Z}/n\mathbf{Z}$ is a cyclic group, then $\mathbf{F}_q[\mathbf{Z}/n\mathbf{Z}] \cong \mathbf{F}_q[x]/\langle x^n - 1 \rangle$; thus, in this case a group algebra code is simply a cyclic code.

An element e in the group algebra R is called an *idempotent* if and only if $e^2 = e$. An idempotent in the center of R is called *central*. Since $\gcd(n,q) = 1$, any R-code is generated by an idempotent, that is, for any left ideal I there exists an idempotent element e in R such that $I = Re$. Two idempotent elements e and f are called *orthogonal* if $ef = 0 = fe$. An nonzero idempotent e in R is called (*centrally*) *primitive* if and only if it cannot be written as the sum of two nonzero orthogonal (central) idempotents in R.

The elements 0 and 1 are idempotents of R. If N is a subgroup of G, then $\widehat{N} = |N|^{-1} \sum_{g \in N} g$ is an idempotent element in the group algebra R. If N is a normal subgroup, then $\widehat{N}$ is a central idempotent. The central idempotent $\widehat{G}$, known as the trivial idempotent, will play a significant role in the subsequent sections. If we multiply an element $b = \sum_{g \in G} b_g g$ by $\widehat{G}$, then we obtain $b\widehat{G} = \left(\sum_{g \in G} b_g \right) \widehat{G}$; in particular, we have $\dim R\widehat{G} = 1$. An element $b = \left(\sum_{g \in G} b_g g \right)$ in R is called *even-like* if and only if $b\widehat{G} = 0$ (viz. $\sum_{g \in G} b_g = 0$). An element of R that is not even-like is called *odd-like*.

An *antiautomorphism* on the group algebra R is a bijective map μ on R that satisfies (i) $\mu(a) + \mu(b) = \mu(a + b)$ and (ii) $\mu(ab) = \mu(b)\mu(a)$ for all a, b in R. We say that the antiautomorphism μ is isometric if it preserves the Hamming weight. An important isometric antiautomorphism on $\mathbf{F}_q[G]$ is μ_{-1} defined as $\mu_{-1}(g) = g^{-1}$ for g in G.

B. Duadic Group Algebra Codes

Let G be a finite group of order n and $\mathbf{F}_q$ a finite field such that $\gcd(q, n) = 1$. If e and f are two even-like idempotents in $R = \mathbf{F}_q[G]$ that satisfy the equations

A1 $e + f = 1 - \widehat{G}$ and

A2 $\mu(e) = f$ and $\mu(f) = e$ for some isometric antiautomorphism μ on R,

then the idempotents e and f generate

C1 a pair of *even-like duadic codes* $C_e := Re$ and $C_f := Rf$,

C2 and a pair of *odd-like duadic codes* $D_e := R(1 - f)$ and $D_f := R(1 - e)$.

The antiautomorphism μ given in **A2** is said to give a splitting. By a slight abuse we also refer to μ_{-1} as a splitting.

Lemma 1: Let G be a group of order n and $\mathbf{F}_q$ a finite field such that $\gcd(n, q) = 1$. If e and f are even-like idempotents in $\mathbf{F}_q[G]$ that satisfy **A1** and **A2** with splitting μ, then we note that

i) the idempotents e, f, and $\widehat{G}$ are pairwise orthogonal;

ii) $\dim C_e = \dim C_f = (n-1)/2$ and $\dim D_e = \dim D_f = (n+1)/2$;

iii) in particular, the order n of the group G must be odd;

iv) the codes satisfy the inclusions $C_e \subseteq D_e$ and $C_f \subseteq D_f$.

Proof: i) Since e and $f = (1 - \widehat{G} - e)$ are even-like, it follows that the idempotents e, f, and $\widehat{G}$ are pairwise orthogonal; hence, $R = Re \oplus Rf \oplus R\widehat{G}$. For ii) and iii), we observe that $\dim R\widehat{G} = 1$ and $\dim Re = \dim R\mu(e) = \dim Rf$, which implies $\dim Re = \dim Rf = (n-1)/2$. The dimensions for the odd-like duadic codes are an immediate consequence, since $C_e \oplus D_f = R$ and $C_f \oplus D_e = R$. For iv), notice that the orthogonality of e and f yields $e(1 - f) = e$ and $f(1 - e) = f$. Therefore, $C_e = Re \subset R(1 - f) = D_e$ and $C_f = Rf \subset R(1 - e) = D_f$. $\blacksquare$

Lemma 2: Let $\mathbf{F}_q$ be a finite field of characteristic p. Suppose that μ is an isometric antiautomorphism of a group algebra $\mathbf{F}_q[G]$ that satisfies $\mu(\widehat{G}) = \widehat{G}$. Then there exists a Galois automorphism $\sigma \in \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$ and an antiautomorphism μ_* of the group G such that

$$\mu(\alpha g) = \sigma(\alpha)\mu_*(g) \quad \text{holds for all } \alpha \in \mathbf{F}_q, g \in G. \quad (1)$$

Proof: The isometry of the antiautomorphism μ implies that the image $\mu(g)$ of an element g in G is of the form $\mu(g) = c_g g'$ for some nonzero constant $c_g \in \mathbf{F}_q$ and $g' \in G$. Since $\mu(\widehat{G}) = \widehat{G}$, we have $c_g = 1$ for all $g \in G$. Therefore, μ restricts to a antiautomorphism μ_* on the group G. Since μ preserves addition and multiplication of scalars and $\mu(\mathbf{F}_q 1) = \mathbf{F}_q 1$, we have $\mu(\alpha 1) = \sigma(\alpha)1$ for some automorphism of $\mathbf{F}_q$. The elements of the prime field $\mathbf{F}_p$ remain fixed, so σ is an element of $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$. The claim is an immediate consequence of these observations. $\blacksquare$

C. Odd-like Weights in Duadic Group Algebra Codes

Our first result is a slight generalization of a theorem by Zhu [14]. We allow isometric antiautomorphisms of $\mathbf{F}_q[G]$, whereas Zhu considers only antiautomorphisms that are induced from the group G.

Lemma 3: Suppose that e and f are idempotents that determine a pair of even-like duadic codes in $\mathbf{F}_q[G]$ with splitting given by μ. If the group G has order n, then the minimum weight d_o of an odd-like element in the odd-like duadic code $D_f = R(1 - e)$ or $D_e = R(1 - f)$ satisfies

i) $d_o^2 \geq n$,

ii) $d_o^2 - d_o + 1 \geq n$ if $\mu = \mu_{-1}$.

Proof: i) Suppose that a is an odd-like element in D_f of weight d_o, so there exists an element $b \in \mathbf{F}_q[G]$ such that $a = b(1-e)$. The element b is odd-like, since $0 \neq a\widehat{G} = b(1-e)\widehat{G} = b\widehat{G}$ holds. A splitting satisfies $\mu(\widehat{G}) = \widehat{G}$; thus, $\mu(b)$ is odd-like as well, as $0 \neq b\widehat{G}$ implies $0 \neq \widehat{G}\mu(b) = \mu(b)\widehat{G}$.

The product of a and $\mu(a)$ has Hamming weight $\leq d_o^2$. However, we recall that $(1 - e)(1 - f) = \widehat{G}$, so

$$a\mu(a) = b(1-e)(1-f)\mu(b) = b\widehat{G}\mu(b) = b\mu(b)\widehat{G} \neq 0.$$

If $b\mu(b) = \sum_{g \in G} c_g g$, then $b\mu(b)\widehat{G} = \left(\sum_{g \in G} c_g\right)\widehat{G}$; thus, the product $a\mu(a)$ yields an element of Hamming weight n, which proves the bound $n \leq d_o^2$.

For part ii), we note that $a\mu_{-1}(a)$ has at most Hamming weight $d_o^2 - d_o + 1$ when a has Hamming weight d_o. By symmetry similar results hold for D_e. $\blacksquare$

D. Duals of Duadic Codes

We can define a *Euclidean inner product* on $\mathbf{F}_q[G]$ by

$$\left\langle \sum_{g \in G} a_g g \middle| \sum_{g \in G} b_g g \right\rangle = \sum_{g \in G} a_g b_g.$$

Lemma 4: Let G be a finite group and $R = \mathbf{F}_q[G]$.

i) The product $ab = 0$ for $a, b \in R$ if and only if $\mu_{-1}(b) \in C^\perp$, where $C = Ra$.

ii) If C is an R-code, then $C^\perp$ is also an R-code.

iii) If e is an idempotent in R and $C = Re$, then $C^\perp = R(1 - \mu_{-1}(e))$.

Proof: i) We note that the product of a and b can be expressed in the form

$$ab = \sum_{g \in G} \left(\sum_{h \in G} a_{gh} b_{h^{-1}} \right) g = \sum_{g \in G} \langle g^{-1}a \mid \mu_{-1}(b) \rangle g,$$

from which we can directly deduce the claim.

ii) We note that the inner product satisfies $\langle ga|gb \rangle = \langle a|b \rangle$ for all g in G and a, b in R. If $a \in C$ and $b \in C^\perp$, then for each $g \in G$, we have $\langle a|gb \rangle = \langle g^{-1}a|b \rangle = 0$, since $g^{-1}a \in C$. Extending linearly shows that $C^\perp$ is a left ideal.

iii) Since $e(1-e) = 0$, property i) shows that the idempotent $1 - \mu_{-1}(e)$ is contained in $C^\perp$, so $R(1-\mu_{-1}(e)) \subseteq C^\perp$ by ii). Since $\dim C^\perp = \dim R(1 - e) = \dim R(1 - \mu_{-1}(e))$, we actually must have equality. $\blacksquare$

Corollary 5: If e and f are even-like idempotents that satisfy **A1** and **A2**, then the following statements hold:

i) If $\mu_{-1}(e) = f$, then $C_e^\perp = D_e$ and $C_f^\perp = D_f$;

ii) if $\mu_{-1}(e) = e$, then $C_e^\perp = D_f$ and $C_f^\perp = D_e$.

III. Existence of Splittings

The goal of this section is to prove the following theorem of the existence of duadic group algebra codes.

Theorem 6: Let G be a finite group of odd order and let $\mathbf{F}_q$ be a finite field with $\gcd(n, q) = 1$. There exists a splitting $\mu = \mu_{-1}$ with central idempotents e and f such that equations **A1** and **A2** are satisfied if and only if the order of q is odd modulo n.

Proof: (Outline) Our proof is subdivided into three parts.

Part A. We show that a splitting μ_{-1} with central idempotents e and f satisfying **A1** and **A2** exists if and only if no nontrivial centrally primitive idempotent is fixed by μ_{-1}, see Proposition 7.

Part B. We then define an action of μ_{-1} on so-called $\mathbf{F}_q$-conjugacy classes in G. We prove that no nontrival centrally primitive idempotent is fixed by μ_{-1} if and only if no $\mathbf{F}_q$-conjugacy class is fixed by the action of μ_{-1}, see Proposition 9.

Part C. By [13, Lemma 2.3], $K \neq \mu_{-1}(K)$ for all nontrivial $\mathbf{F}_q$-conjugacy classes K if and only the order of q is odd modulo n.

The claim follows by combining the three parts. ∎

Actually, our proofs of **Part A** and **Part B** are valid for arbitrary splittings μ. If one can find necessary and sufficient conditions such that $\mu(K) \neq K$ holds for all nontrival $\mathbf{F}_q$-conjugacy classes, then one already obtains an extension of the theorem to μ-splittings.

One technical difficulty in our proof is that the counting argument used in **Part B** cannot be done in nonzero characteristic. We circumvent this problem by using an extension of the field of p-adic integers (a local field) such that the ring of integers in this field reduces to the given finite field modulo its maximal ideal; this proof technique is interesting in itself.

Part A. We now supply the details of **Part A** of the proof.

Proposition 7: There exists a splitting μ with even-like (central) idempotents e and f that satisfy **A1** and **A2** if and only if each nontrivial (centrally) primitive idempotent h of $\mathbf{F}_q[G]$ satisfies $\mu(h) \neq h$.

Proof: Suppose that e and f are even-like (central) idempotents that satisfy **A1** and **A2**. These equations imply that $e + f + \widehat{G} = 1$, where the idempotents e, f, and $\widehat{G}$ are pairwise orthogonal. Suppose that $e = h_1 + \cdots + h_m$ is a decomposition of the idempotent e into orthogonal (centrally) primitive idempotents. Seeking a contradiction, we assume that $\mu(h_k) = h_k$ for some k in the range $1 \leq k \leq m$. However, then e and f cannot be orthogonal idempotents, contradiction.

Conversely, suppose that $h \neq \mu(h)$ for all nontrivial primitive (central) idempotents h of $\mathbf{F}_q[G]$. Partition the nontrivial (central) primitive idempotents into disjoint pairs $\{h_1, \mu(h_1)\}, \ldots, \{h_\ell, \mu(h_\ell)\}$. Let $e = h_1 + \cdots + h_\ell$ and $f = \mu(e)$. Then $e + f = 1 - \widehat{G}$ and $e\widehat{G} = 0$ and $f\widehat{G} = 0$. Further, $\mu(e + f + \widehat{G}) = 1 = e + f + \widehat{G}$ implies that $e = \mu(f)$. So μ is the desired splitting with (central) even-like idempotents e and f. ∎

Part B. The second part of our argument is more involved. Our goal is to prove the key proposition below. However,

we need some preparation to state this result. We note that a centrally primitive idempotent e_χ of $\mathbf{F}_q[G]$ can be explicitly written in the form

$$e_\chi = \frac{n_\chi}{|G|} \sum_{g \in G} \chi(g) g^{-1}, \tag{2}$$

where χ is an irreducible $\mathbf{F}_q$-character and n_χ is a positive integer that depends on χ, see Lemma 14 in the Appendix.

Lemma 8: Let $\mathbf{F}_q$ be a finite field and G a finite group of order n such that $\gcd(n, q) = 1$. Suppose that μ is an antiautomorphism of $\mathbf{F}_q[G]$ of the form (1). Then the action of μ on a centrally primitive idempotent (2) is given by

$$\mu(e_\chi) = \frac{n_\chi}{|G|} \sum_{g \in G} \chi(\mu_*^{-1}(g^k)) g^{-1},$$

where k is a positive integer determined by the Galois automorphism σ and μ_*^{-1} is the inverse of the group antiautomorphism μ_*. In particular, k is a power of the characteristic of $\mathbf{F}_q$.

Proof: If the exponent of the group G is m, then the values of the character are contained in $\mathbf{F}_q \cap \mathbf{F}_p(\delta)$, where δ is a primitive m-th root of unity over the prime field $\mathbf{F}_p$. Suppose that σ' is a Galois automorphism of $\mathrm{Gal}(\mathbf{F}_q(\delta)/\mathbf{F}_p)$ that restricts to the Galois automorphism σ on $\mathbf{F}_q$. If $\sigma'(\delta) = \delta^k$, then $\sigma(\chi(g)) = \chi(g^k)$ holds for all g in G, and the action of an antiautomorphism μ is given by

$$\mu(e_\chi) = \frac{n_\chi}{|G|} \sum_{g \in G} \sigma(\chi(g)) \mu_*(g^{-1}) = \frac{n_\chi}{|G|} \sum_{g \in G} \chi(\mu_*^{-1}(g^k)) g^{-1},$$

where the latter equality is obtained by substituting $\mu_*^{-1}(g)$ for g. ∎

Let us recall the concept of an $\mathbf{F}_q$-conjugacy class before stating our next result. The $\mathbf{F}_q$-conjugacy class $K_q(g)$ of an element g in a finite group G is the set

$$K_q(g) = \{h^{-1} g^{q^k} h \mid h \in G, k \geq 0\}.$$

It is easy to see that two $\mathbf{F}_q$-conjugacy classes are either disjoint or coincide. The following two key facts are essential for our purpose: (i) An irreducible $\mathbf{F}_q$-character is constant on $\mathbf{F}_q$-conjugacy classes, and (ii) the number of $\mathbf{F}_q$-conjugacy coincides with the number of irreducible $\mathbf{F}_q$-characters.

We define an action of an antiautomorphism μ of the form (1) on an $\mathbf{F}_q$-conjugacy class $K_q(g)$ by

$$K_q^\mu(g) = K_q(\mu_*(g)^\ell),$$

where ℓ is a positive integer such that $k\ell \equiv 1 \bmod m$, k is the integer given in Lemma 8, and m is the exponent of the group G.

Proposition 9 (Key Proposition): Let $\mathbf{F}_q$ be a finite field and let G be a finite group of order n such that $\gcd(n, q) = 1$. If μ is an antiautomorphism of $\mathbf{F}_q[G]$ of the form (1), then the number of $\mathbf{F}_q$-conjugacy classes of G that are fixed by μ coincides with the number of centrally primitive idempotents of $\mathbf{F}_q[G]$ that are fixed by μ.

Proof: *Step 1.* Suppose that the finite field $\mathbf{F}_q$ has characteristic p. There exists a monic irreducible polynomial

$f(x)$ in $\mathbf{F}_p[x]$ such that $\mathbf{F}_p[x]/\langle f(x)\rangle = \mathbf{F}_q$. Let $\mathbf{Z}_p$ denote the ring of p-adic integers and $\mathbf{Q}_p$ its quotient field. Then $\mathfrak{p} = p\mathbf{Z}_p$ is the unique nonzero prime ideal of $\mathbf{Z}_p$ and $\mathbf{Z}_p/\mathfrak{p} \cong \mathbf{F}_p$. Choose a monic polynomial $g(x)$ in $\mathbf{Z}_p[x]$ such that $f(x) \equiv g(x) \bmod \mathfrak{p}$. Then $R = \mathbf{Z}_p[x]/\langle g(x)\rangle$ is a discrete valuation ring with nonzero prime ideal $\mathfrak{P} = \mathfrak{p}R$.

If K denotes the field $\mathbf{Q}_p[x]/\langle g(x)\rangle$, then $K/\mathbf{Q}_p$ is an unramified Galois extension. The Galois group $\mathrm{Gal}(K/\mathbf{Q}_p)$ can be identified with the cyclic group $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$. The latter group is generated by the automorphism $x \mapsto x^p$, and the generator of $\mathrm{Gal}(K/\mathbf{Q}_p)$ can be characterized by

$$b \equiv b^p \bmod \mathfrak{P} \quad \text{for all} \quad b \in R.$$

All facts stated in this step are proved in [8, Chapter 1].

Step 2. The number of centrally primitive idempotents in $K[G]$ and in $\mathbf{F}_q[G]$ is the same. If Y denotes the set of irreducible K-characters of G, then the set of centrally primitive idempotents $\{e_\chi \mid \chi \in Y\}$ of $K[G]$ is bijectively mapped to the centrally primitive idempotents of $\mathbf{F}_q[G]$ by reduction modulo $\mathfrak{P}$.

Let k be the integer defined as in Lemma 8. Then there exists a unique automorphism τ in $\mathrm{Gal}(K/\mathbf{Q}_p)$ such that $\tau(x) = x^k \bmod \mathfrak{P}$. Therefore, we can define an antiautomorphism η on $K[G]$ by $\eta(\alpha g) = \tau(\alpha)\mu_*(g)$ such that

$$\eta(e_\chi) \bmod \mathfrak{P} = \mu(e_\chi \bmod \mathfrak{P}) \tag{3}$$

holds for all centrally primitive idempotents e_χ of $K[G]$. The latter equation guarantees that the number of idempotents in $K[G]$ fixed by η is the same as the number of idempotents in $\mathbf{F}_q[G]$ fixed by μ.

Step 3. A centrally primitive idempotent in $K[G]$ is of the form

$$e_\chi = \frac{n_\chi}{|G|} \sum_{g \in G} \chi(g)g^{-1}.$$

It follows from Lemma 8 that $\eta(e_\chi) = e_\chi$ if and only if $\chi(g) = \chi(\eta^{-1}(g^k))$ holds for all g in G. Therefore, we define the action of η on an irreducible K-character by

$$\chi^\eta(g) = \chi(\mu_*^{-1}(g^k)), \tag{4}$$

for all g in G.

An irreducible K-character is constant on K-conjugacy classes. The K-conjugacy classes coincide with the $\mathbf{F}_q$-conjugacy classes, since the Galois groups are isomorphic. Suppose that m is the exponent of the group G. There exists a positive integer ℓ such that $k\ell \equiv 1 \bmod m$. We define the action of η on $\mathbf{F}_q$-conjugacy classes by

$$K_q^\eta(g) = K_q(\mu_*(g^\ell)), \tag{5}$$

for all g in G. The definitions are carefully chosen such that

$$\chi^\eta(K_q^\eta(g)) = \chi(K_q(g))$$

holds for all g in G.

Step 4. Let K_q denote the set of $\mathbf{F}_q$-conjugacy classes. We have $|Y| = |K_q|$. Therefore, we can define the square matrix

$$U = (\chi(K))_{\chi \in Y, K \in K_q}.$$

We note that U is nonsingular, since the irreducible K-characters are linearly independent over K. Let $A = (A_{\chi,\psi})_{\chi,\psi \in Y}$ and $B = (B_{L,K})_{L,K \in K_q}$ be permutation matrices that are respectively defined by

$$A_{\chi,\psi} = \begin{cases} 1 & \text{if } \chi = \psi^\eta \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad B_{L,K} = \begin{cases} 1 & \text{if } K^\eta = L \\ 0 & \text{otherwise.} \end{cases}$$

Since $\chi^\eta(K^\eta) = \chi(K)$, we have

$$\sum_{\psi \in Y} A_{\chi,\psi}\psi(K) = \chi(K^\eta) \quad \text{and} \quad \sum_{L \in K_q} \chi(L)B_{L,K} = \chi(K^\eta),$$

so $AU = UB$. Since U is invertible, we have $A = UBU^{-1}$. Thus, $\mathrm{tr}(A) = \mathrm{tr}(B)$. The trace of A counts the number of characters that remain fixed under the action of η, and the trace of B counts the number of $\mathbf{F}_q$-conjugacy classes that remain fixed under η. These facts imply the claim. ∎

Recall that **Part C** has been proved in [13]; thus, this concludes our proof of Theorem 6. For the existence of duadic group algebra codes with splitting $\mu \neq \mu_{-1}$ one only needs to modify **Part C**.

IV. EXTENSIONS AND APPLICATIONS

The natural question following the previous section is the existence of duadic group algebra codes when the order of q is even. The splitting is no longer given by μ_{-1}, but we will show that there exist duadic algebra codes. We will confine ourselves to the abelian case. Then we will give an application of duadic group algebra codes to quantum error-correction.

A. Extensions

Cyclic duadic codes exist if and only if q is a quadratic residue modulo n. However, this condition is not required for group codes. We partially generalize some of the existence results of [7], where characteristic two is considered.

Lemma 10: Let $G = \langle a,b \mid a^p = b^p = 1, ab = ba\rangle$, where p is an odd prime and q be a prime power such that $\mathrm{ord}_p(q)$ is even and $\gcd(p,q) = 1$. The $\mathbf{F}_q$-conjugacy class of an element $a^x b^y$ in G is given by $C_{x,y}^{(q)} = \{a^{xq^j} b^{yq^j} \mid j \in \mathbf{Z}\}$. Then the automorphism μ defined as $\mu(a^x b^y) = a^{qy} b^x$ does not fix any of the $\mathbf{F}_q$-conjugacy classes if $(x,y) \neq (0,0)$. Further, μ_{-1} fixes each $\mathbf{F}_q$-conjugacy class *i.e.*, $\mu_{-1}(C_{x,y}^{(q)}) = C_{x,y}^{(q)}$.

Proof: Assume that there is an element $a^x b^y \in G$, such that $\mu(C_{x,y}^{(q)}) = C_{x,y}^{(q)}$. Then there exists an integer j such that $\mu(a^x b^y) = a^{xq^j} b^{yq^j}$. This implies that $(qy,x) = (xq^j, yq^j) \bmod p$ or $qy \equiv xq^j \bmod p$ and $x \equiv yq^j \bmod p$. If $x = 0, y \neq 0$, then we have $qy \equiv 0 \bmod p$ or $y = 0$; a contradiction. If $y = 0, x \neq 0$, then it follows $x = 0$, which leads to a contradiction again. Assuming that both $x, y \neq 0$ we get $qxy \equiv xyq^{2j} \bmod p$. Since q,x,y are all coprime to p this can be written as $1 \equiv q^{2j-1} \bmod p$. But as $\mathrm{ord}_p(q)$ is even, $1 \not\equiv q^{2j-1} \bmod p$. Therefore, none of the $\mathbf{F}_q$-conjugacy classes are fixed by μ. Let $\mathrm{ord}_p(q) = 2w$, then $q^{2w} \equiv 1 \bmod p$, which implies that $q^w \equiv -1 \bmod p$. Hence, $C_{x,y}^{(q)} = C_{-x,-y}^{(q)} = \mu_{-1}(C_{x,y}^{(q)})$. ∎

Theorem 11: Let $G = \langle a,b \mid a^p = b^p = 1, ab = ba\rangle$ with p an odd prime, q a prime power, $\gcd(p,q) = 1$ and $\mathrm{ord}_p(q)$

even. Then there exist duadic codes over $\mathbf{F}_q[G]$ with splitting given by μ where $\mu(a^x b^y) = a^{qy} b^x$ for any element $a^x b^y \in G$. These codes are fixed by μ_{-1}.

Proof: By **Part A** (Proposition 7), **Part B** (Proposition 9), and replacing **Part C** by Lemma 10, we know that there exist a pair of duadic codes over $\mathbf{F}_q[G]$ with splitting given by μ such that the codes are fixed by μ_{-1}. ∎

B. Quantum Error-Correction

Quantum codes can be utilized to protect quantum information over noisy quantum channels. The CSS construction is particularly transparent method to derive quantum stabilizer codes from a pair of classical codes.

Lemma 12 (CSS Construction [2], [11]): Suppose that C and D are linear codes over a finite field $\mathbf{F}_q$ such that $C \subseteq D$. If C is an $[n, k_1]_q$ code and D an $[n, k_2]_q$ code, then there exists an $[[n, k_2 - k_1, d]]_q$ stabilizer code with minimum distance $d = \min \operatorname{wt}\{(D \setminus C) \cup (C^\perp \setminus D^\perp)\}$.

Theorem 13: Let n be an odd positive integer and q a power of a prime such that the order of q modulo n is odd. Then there exists an $[[n, 1, d]]_q$ stabilizer code with $d^2 - d + 1 \geq n$.

Proof: There exists a group G of order n. By Theorem 6, there exist idempotents e and f in $\mathbf{F}_q[G]$ that satisfy **A1** and **A2** with splitting given by $\mu = \mu_{-1}$. By Lemma 1, we have $C_e \subset D_e$. The CSS construction shows that there exists an $[[n, (n+1)/2 - (n-1)/2, d]]_q = [[n, 1, d]]_q$ stabilizer code with minimum distance $d = \min\{(D_e \setminus C_e) \cup (C_e^\perp \setminus D_e^\perp)\} = \min\{(D_e \setminus C_e) \cup (D_e \setminus C_e)\}$, where the latter equality follows from Corollary 5 i). Since $D_e = R\widehat{G} \oplus C_e$, we observe that $D_e \setminus C_e$ contains precisely the odd-like elements of D_e. By Lemma 3, the minimum weight of an odd-like element in D_e satisfies $d^2 - d + 1 \geq n$. ∎

The distance of the quantum codes does not depend on $\operatorname{wt}(C)$ or $\operatorname{wt}(D)$ or even their dual distances, rather the set differences $D \setminus C$ and $C^\perp \setminus D^\perp$. This means that a code that is bad in the classical sense can lead to a good quantum code, if only we can arrange the low weight codewords of D to be entirely in C and similarly for the low weight codewords of $C^\perp$ to be in $D^\perp$; this phenomenon is called degeneracy. A nice consequence of degeneracy is that errors in C or $D^\perp$ do not require any error-correction, which is a desirable feature as quantum error-correction can be faulty. Thus we require many likely errors to be in C and $D^\perp$. Of course, it is difficult to construct codes that satisfy this strange requirement.

Duadic group algebra codes can meet these conflicting requirements, because their odd-like distance grows with the length n, while we can design their even-like distance to be very small. In [1], we showed how this can be done for cyclic duadic codes over $\mathbf{F}_q$. These codes exists if and only if q is a quadratic residue modulo n. Duadic group algebra codes on the other hand enable us to overcome this restriction.

Now we will give some evidence of the usefulness of the group algebra codes, by constructing a degenerate $[[81, 1, \geq 9]]_2$ quantum code which has many codewords of weight 4. Let $G_i = \mathbf{Z}_3 \times \mathbf{Z}_3 = \langle a_i, b_i \mid a_i^3 = b_i^3 = 1, a_i b_i = b_i a_i \rangle$, then from Theorem 11 we know that there exist duadic group algebra

codes over $\mathbf{F}_2[G_i]$ with idempotents $e_i = a_i + a_i^2 + a_i b_i + a_i^2 b_i^2$ and $f_i = b_i + b_i^2 + a_i b_i^2 + a_i^2 b_i$ satisfying **A1** and **A2**, under the action of $\mu_i(a_i^x b_i^y) = a_i^{2y} b_i^x$. Further e_i, f_i are fixed by μ_{-1}.

We can construct a duadic code over $\mathbf{F}_2[G_1 \times G_2]$ using a construction similar to [7, Theorem 5.6]. Embedding G_i into $G_1 \times G_2$, we get the idempotents of the new code as $e = e_1 + e_2 - e_1 e_2 - f_1 e_2$ and $f = f_1 + f_2 - f_1 f_2 - e_1 f_2$. The splitting for this code is given by $\mu = \mu_1 \times \mu_2$.

These idempotents give us duadic group algebra codes over $\mathbf{F}_2[G_1 \times G_2]$ that are fixed by μ_{-1}. As $e e_1 = e_1$, $\operatorname{wt}(C_e) = \operatorname{wt}(C_f) \leq \operatorname{wt}(e_1) = 4$, while $\operatorname{wt}(D_e \setminus C_e) = \operatorname{wt}(C_e^\perp \setminus D_e^\perp) = \operatorname{wt}(D_f \setminus C_f) \geq 9$ by Corollary 5 ii) and Lemma 3. Thus by Lemma 12 there exists a $[[81, 1, \geq 9]]_2$ quantum code; this code is degenerate and many errors of weights between 4 and 9 (contained in C_e or $D_e^\perp$) do not need error-correction.

APPENDIX

Lemma 14: Let G be a finite group of order n and F a finite field of characteristic coprime to n. If $E \supseteq F$ is a splitting field for G, W an irreducible FG-modul affording the character χ, and V an irreducible submodul of the EG-modul $E \otimes W$ affording the character θ, then $\chi(x) = \sum_{\sigma \in H} \theta^\sigma(x)$, where $H = \operatorname{Gal}(\mathbf{F}_q(\theta)/\mathbf{F}_q)$, and $e = \frac{\theta(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$ is a centrally primitive idempotent in FG.

Proof: Since F is a finite field, we note that the Schur index of the character θ is 1 by [3, Theorem 24.10]. Therefore, the character χ is of the claimed form by [3, Theorem 24.14]. We note that $e_\theta = \frac{\theta(1)}{|G|} \sum_{g \in G} \theta(g^{-1})g$ is a centrally primitive idempotent of EG by [3, Lemma 24.13]. The form of the character χ implies that $e = \sum_{\sigma \in H} e_{\theta^\sigma}$, so e is a central idempotent of FG. The primitivity of e is shown in [4, Theorem 19.2.9]. ∎

REFERENCES

[1] S.A. Aly, A. Klappenecker, and P. Sarvepalli. Remarkable degenerate quantum stabilizer codes derived from duadic codes. In *Proc. 2006 IEEE ISIT, Seattle, USA*, pages 1114–1118, 2006.

[2] A.R. Calderbank and P. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996.

[3] L. Dornhoff. *Group Representation Theory*, volume Part A. Marcel Dekker, New York, 1971.

[4] G. Karpilovsky. *Group Representations*, volume I, Part B. North-Holland, Amsterdam, 1992.

[5] J.S. Leon, J.M. Masley, and V. Pless. Duadic codes. *IEEE Trans. Inform. Theory*, 30(5):709–714, 1984.

[6] J. MacWilliams. Codes and ideals in group algebra. *Combinatorial Mathematics and its applications*, ch. 18, Univ. of North Carolina Press, Chapel Hill, 1969.

[7] J.J. Rushanan. *Topics in Integral Matrices and Abelian Group Codes*. PhD thesis, California Institute of Technology, 1986.

[8] J.-P. Serre. *Local Fields*. Springer-Verlag, New York, 2nd corrected printing edition, 1995.

[9] M.H.M. Smid. On duadic codes. Master's thesis, Dept. Math., Tech. Univ. Einhoven, Netherlands, 1986.

[10] M.H.M. Smid. Duadic codes. *IEEE Trans. Inform. Theory*, 3:432–433, 1987.

[11] A.M. Steane. Simple quantum error correcting codes. *Phys. Rev. Lett.*, 77:793–797, 1996.

[12] H.N. Ward and L. Zhu. Existence of abelian group code partitions. *J. Combin. Theory Ser. A*, 67:276–281, 1994.

[13] S. Zhang. Existence of certain class of duadic group algebra codes. *J. Stat. Plann. Inf.*, 94:405–411, 2001.

[14] L. Zhu. Duadic group algebra codes. *J. Stat. Plann. Inf.*, 51:395–401, 1996.